**EBS**

* SSD-backed storage for transactional workloads and HDD-backed storage for throughput intensive workloads.
* To maximize the performance of st1 and sc1, we recommend using [EBS-optimized EC2 instances](https://aws.amazon.com/ebs/features/#Amazon_EBS-Optimized_instances).
* Q: What is Amazon EBS encryption?
* Amazon EBS encryption offers seamless encryption of EBS data volumes, boot volumes and snapshots, eliminating the need to build and maintain a secure key management infrastructure. EBS encryption enables data at rest security by encrypting your data using Amazon-managed keys, or keys you create and manage using the [AWS Key Management Service (KMS)](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys). The encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage
* Q: What is the AWS Key Management Service (KMS)?
* [AWS KMS](https://aws.amazon.com/kms/) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS Key Management Service is integrated with other AWS services including Amazon EBS, Amazon S3, and Amazon Redshift, to make it simple to encrypt your data with encryption keys that you manage. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
* : How are my Amazon EBS encryption keys managed?
* Amazon EBS encryption handles key management for you. Each newly created volume gets a unique 256-bit AES key; Volumes created from the encrypted snapshots share the key. These keys are protected by our own key management infrastructure, which implements strong logical and physical security controls to prevent unauthorized access. Your data and associated keys are encrypted using the industry-standard AES-256 algorithm
* Q: Can I create an encrypted data volume at the time of instance launch?
* Yes, using [customer master keys (CMKs)](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys) that are either AWS-managed or customer-managed. You can specify the volume details and encryption through a [RunInstances API](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_RunInstances.html) call with the [BlockDeviceMapping](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_BlockDeviceMapping.html) parameter or through the Launch Wizard in the EC2 Console.
* Q: Can I launch an encrypted EBS instance from an unencrypted AMI?
* Yes
* Q: Can I share encrypted snapshots and AMIs with other accounts?
* Yes. You can share encrypted snapshots and AMIs using a [customer-managed customer master key (CMK)](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html) with other AWS accounts
* Q: Can I ensure that all new volumes created are always encrypted?
* Yes, you can enable EBS encryption by default with a single setting per region. This ensures that all new volumes are always encrypted.
* Q: How do I modify the capacity, performance, or type of an existing EBS volume?
* Changing a volume configuration is easy. The [Elastic Volumes](https://aws.amazon.com/ebs/features/#Amazon_EBS_Elastic_Volumes) feature allows you to increase capacity, tune performance, or change your volume type with a single CLI call, API call or a few console clicks.
* Q: Does the I/O size of my application reads and writes affect the rate of throughput I get from my HDD-backed volumes?
* Yes. The throughput rate you get depends on the I/O size of your application reads and writes. HDD-backed volumes process reads and writes in I/O sizes of 1MB. Sequential I/Os are merged and processed as 1 MB units while each non-sequential I/O is processed as 1MB even if the actual I/O size is smaller. Thus, while a transactional workload with small, random IOs, such as a database, won't perform well on HDD-backed volumes, sequential I/Os and large I/O sizes will achieve the advertised performance of st1 and sc1 for a longer period of time
* Q: Is there an additional fee to enable Multi-Attach?
* No. Multi-Attach can be enabled on an EBS Provisioned IOPS io1 volume and there will be charges for the storage (GB-Mo) and IOPS (IOPS-Mo) provisioned.
* Q: Can I boot an EC2 instance using a Multi-Attach enabled volume?
* No
* Q: What happens if all of my attached instances do not have the ‘deleteOnTermination’ flag set?
* The volume's deleteOnTermination behavior is determined by the configuration of the last attached instance that is terminated. To ensure predictable delete on termination behavior, enable or disable 'deleteOnTermination' for all of the instances to which the volume is attached.
* If you want the volume to be deleted when the attached instances are terminated, enable ‘deleteOnTermination’ for all of instances to which the volume is attached. If you want to retain the volume after the attached instances have been terminated, disable ‘deleteOnTermination’ for all attached instances. For more information, see [Multi-Attach](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html) technical documentation.
* Q: Can my application use Multi-Attach?
* If your application does not require storage layer coordination of write operations, such as a read-only application or it enforces application level IO fencing, then your application can use Multi-Attach.
* **Q: Do you support multiple instances accessing a single volume?**
* Yes, you can enable Multi-Attach on an EBS Provisioned IOPS io1 volume to allow a volume to be concurrently attached to up to sixteen Nitro-based EC2 instances within the same Availability Zone.
* **Q: Will I be able to access my EBS snapshots using the regular Amazon S3 APIs?**
* EBS snapshots are only available through the Amazon EC2 APIs.
* **Q: Do volumes need to be un-mounted in order to take a snapshot? Does the snapshot need to complete before the volume can be used again?**
* No, snapshots can be done in real time while the volume is attached and in use. However, snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or OS. In order to ensure consistent snapshots on volumes attached to an instance, we recommend cleanly detaching the volume, issuing the snapshot command, and then reattaching the volume. For Amazon EBS volumes that serve as root devices, we recommend shutting down the machine to take a clean snapshot.
* **Q: Are snapshots versioned? Can I read an older snapshot to do a point-in-time recovery?**
* Each snapshot is given a unique identifier, and customers can create volumes based on any of their existing snapshots.
* **Q: What charges apply when using Amazon EBS shared snapshots?**
* If you share a snapshot, you won’t be charged when other users make a copy of your snapshot. If you make a copy of another user’s shared volume, you will be charged normal EBS rates.
* **Q: Can users of my Amazon EBS shared snapshots change any of my data?**
* Users who have permission to create volumes based on your shared snapshots will first make a copy of the snapshot into their account. Users can modify their own copies of the data, but the data on your original snapshot and any other volumes created by other users from your original snapshot will remain unmodified.
* **Q: How can I discover Amazon EBS snapshots that have been shared with me?**
* You can find snapshots that have been shared with you by selecting “Private Snapshots” from the viewing dropdown in the Snapshots section of the AWS Management Console. This section will list both snapshots you own and snapshots that have been shared with you.
* **Q: How can I find what Amazon EBS snapshots are shared globally?**
* You can find snapshots that have been shared globally by selecting “Public Snapshots” from the viewing dropdown in the Snapshots section of the AWS Management Console.
* **Q: Since io2 provides higher volume durability, should I still take snapshots and plan to replicate io2 volumes across Availability Zones (AZs) for high durability?**
* High volume durability, snapshots, and replicating volumes across AZs protect against different types of failures, and customers can choose to use one, two, or all of these approaches based on their data durability requirements. Higher volume durability reduces the probability of losing the primary copy of your data. Snapshots protect against the unlikely event of a volume failure. Replicating volumes across AZs protects against an AZ level failure and also provides faster recovery in case of failure.
* **Q: Can I stripe multiple volumes together to get better performance?**
* Yes. You can stripe multiple volumes together to achieve up to 260,000 IOPS or 60,000 Mbps (or 7500 MB/s) when attached to larger EC2 instances. However, performance for st1 and sc1 scales linearly with volume size so there may not be as much of a benefit to stripe these volumes togeth
* **Q. What is EBS Block Express?**
* EBS Block Express is the next generation of Amazon EBS storage server architecture purpose-built to deliver the highest levels of performance with sub-millisecond latency for block storage at cloud scale. Block Express does this by using Scalable Reliable Datagrams (SRD), a high-performance lower-latency network protocol, to communicate with Nitro System-based EC2 instances
* **Q: Does it take longer to snapshot an entire 16 TB volume as compared to an entire 1 TB volume?**
* By design, an EBS Snapshot of an entire 16 TB volume should take no longer than the time it takes to snapshot an entire 1 TB volume. However, the actual time taken to create a snapshot depends on several factors including the amount of data that has changed since the last snapshot of the EBS volume.
* **Q: When would I use Fast Snapshot Restore (FSR)?**
* You should enable FSR on snapshots if you are concerned about latency of data access when you restore data from a snapshot to a volume and want to avoid the initial performance hit during initialization. FSR is intended to help with use cases such as virtual desktop infrastructure (VDI), backup & restore, test/dev volume copies, and booting from custom AMIs. By enabling FSR on your snapshot, you will see improved and predictable performance whenever you need to restore data from that snapshot.
* **Q: Does enabling FSR for my snapshot speed up snapshot creation?**
* No. FSR-enabled snapshots improve restoring backup data from your snapshot to your volumes. FSR-enabled snapshots do not speed up snapshot creation time.
* **Q: How do I enable Fast Snapshot Restore (FSR)?**
* To use the feature, invoke the new enable-fast-snapshot-restores API on a snapshot within the availability zone (AZ) where initialized volumes are to be restored.
* When you delete a snapshot, the FSR for your snapshot is automatically disabled and FSR billing for the snapshot will be terminated.
* **Q: Can I create an encrypted data volume at the time of instance launch?**
* Yes, using [customer master keys (CMKs)](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys) that are either AWS-managed or customer-managed. You can specify the volume details and encryption through a [RunInstances API](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_RunInstances.html) call with the [BlockDeviceMapping](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_BlockDeviceMapping.html) parameter or through the Launch Wizard in the EC2 Console.
* **Q: Can I create additional encrypted data volumes at the time of instance launch that are not part of the AMI?**
* Yes, you can create encrypted data volume with either default or custom CMK encryption at the time of instances launch. You can specify the volume details and encryption through [BlockDeviceMapping](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_BlockDeviceMapping.html) object in [RunInstances API](http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_RunInstances.html) call or through Launch Wizard in EC2 Console.
* **Q: Can I ensure that all new volumes created are always encrypted?**
* Yes, you can enable EBS encryption by default with a single setting per region. This ensures that all new volumes are always encrypted. Refer to [technical documentation](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html) for more details.
* **200 GiB size volume with 15000 IOPS** - This is an incorrect configuration. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. So, for a 200 GiB volume size, max IOPS possible is 20\*50 = 10000 IOPS.
* Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices.
* You can mount these volumes as devices on your instances. You can mount multiple volumes on the same instance, and you can mount a volume to multiple instances at a time.
* You can create a file system on top of these volumes or use them in any way you would use a block device (like a hard drive). You can dynamically change the configuration of a volume attached to an instance.
* The simplest solution for this scenario is to choose a local Elastic Block Store (EBS) volume to write the log files to. This requires no additional coding.
* Write the log files to an attached Amazon EBS volume" is the correct answer.
* "Write the log files to an Amazon S3 bucket" is incorrect as this is not the simplest solution as it would require additional code in the application compared to just writing the data to a local volume.